GENERATING TRANSITIVE PERMUTATION GROUPS

By L. G. KOVÁCS and M. F. NEWMAN

[Received 10th June 1987]

1. Our aim is to prove the following.

THEOREM. *There is a constant c such that for each positive integer $d(\geqslant 2)$, each nilpotent transitive group of degree d can be generated by $[cd(\log d)^{-\frac{1}{2}}]$ elements. Moreover for each prime p there is a positive constant c_p such that whenever d is a power of p there is a transitive p-group of degree d which cannot be generated by $[c_p d(\log d)^{-\frac{1}{2}}]$ elements.*

It is tempting to conjecture that this remains true with "nilpotent" deleted. The group-theoretic part of our proof does not seem good enough for an attempt to find the optimal constants, so we shall not trouble to polish the calculus or extract precise numerical values from our arguments.

2. For each prime power p^n, let $f(p^n)$ denote the least integer such that each transitive p-group of degree p^n can be generated by $f(p^n)$ elements. Further, let $M(p^n)$ denote the coefficient of $x^{[(p-1)n/2]}$ in the polynomial $(1+x+\cdots+x^{p-1})^n$. The bulk of the paper will be taken up by proving that

$$\frac{1}{p}M(p^n) \leqslant f(p^n) \leqslant \frac{2}{p-1}M(p^n) \quad \text{whenever } n>1. \tag{2.1}$$

Since $M(2^n)$ is a binomial coefficient, Stirling's Formula yields that $M(2^n)$ is asymptotically a constant multiple of $2^n n^{-\frac{1}{2}}$. We are grateful to Professors Kurt Mahler and Sir Peter Swinnerton-Dyer for showing us how to prove (for p odd) that

(2.2) $M(p^n)$ is asymptotically a constant multiple of $p^n n^{-\frac{1}{2}}$.

In view of the first half of (2.1), this implies that suitable c_p always exist.

A simpler version of their argument yields that

$$M(p^n) < 2p^n n^{-\frac{1}{2}} \quad \text{for all } p^n. \tag{2.3}$$

The existence of a suitable c then also follows. Indeed, let G be a nilpotent transitive group of degree d, take a point stabilizer G_0 in G, write the prime-power factorization of d as $d=\prod p^{n(p)}$, let G_p range through the Sylow subgroups of G, and argue as follows. The group G is

the direct product of the G_p, and G_0 is the direct product of the intersections $G_0 \cap G_p$. The index $|G: G_0|$ is d, and $|G_p: (G_0 \cap G_p)| = p^{n(p)}$. Since G_0 is corefree in G, each $G_0 \cap G_p$ is corefree in the relevant G_p. Thus G_p has a faithful transitive permutation representation of degree $p^{n(p)}$, and hence it can be generated by $f(p^{n(p)})$ elements. Consequently, G can be generated by $\max f(p^{n(p)})$ elements. Since $d(\log d)^{-\frac{1}{2}}$ is monotone increasing, by (2.1) and (2.3) we have

$$f(p^{n(p)}) \leqslant \frac{2}{p-1} M(p^{n(p)}) < \frac{4}{p-1} p^{n(p)}(n(p))^{-\frac{1}{2}} \leqslant 4d(\log d)^{-\frac{1}{2}}.$$

It would be easy enough to improve (2.1) a little. Indeed, its first inequality comes from the slightly sharper

$$(n-1) + M(p^{n-1}) \leqslant f(p^n): \tag{2.4}$$

in (2.1) we preferred to compare f and M "pointwise". The second inequality in (2.1) is proved by induction on n, the critical step being

$$f(p^n) \leqslant f(p^{n-1}) + M(p^{n-1}): \tag{2.5}$$

this could also be used a bit more effectively. However, we feel that (2.4) and (2.5) are already far too generous, anyway.

The inequality (2.4) is contained in the unpublished part of Audu's thesis [2], with essentially the same proof as we give here. Our "re-discovery" might have been inspired by our having heard of his work in a 1983 lecture by Dr P. M. Neumann; we are indebted to him for this reference. He has also drawn our attention to the paper [5] of Ronse, in which it was shown that

$$f(p^n) \leqslant 1 + (p^{n-1} - 1)/(p-1).$$

3. The coefficients $M(p^n)$ are relevant here because of the following combinatorial interpretation. Set

$$(1 + x + \cdots + x^{p-1})^n = \sum u(m, n) x^m,$$

so $M(p^n) = u([(p-1)n/2], n)$. In the (commutative) polynomial algebra $\mathbb{Z}[x_1, \ldots, x_n]$, consider the p^n monomials which have degree less than p in each indeterminate. Ordered by divisibility (in the multiplicative semigroup of monomials), they form a poset P_n, which is a cartesian product of the chains $\{1, x_i, \ldots, x_i^{p-1}\}$. The subset consisting of the monomials of total degree m is called level m of P_n; it is obviously an antichain. The information we need is that no antichain in P_n is larger than level $[(p-1)n/2]$ (de Bruijn *et al.* [3]; see also Aigner [1] VIII.3); in particular, no other level is larger. The sum of the elements of P_n is $\prod (1 + x_i + \cdots + x_i^{p-1})$, and the homomorphism $\mathbb{Z}[x_1, \ldots, x_n] \to \mathbb{Z}[x]$

which drops the subscript off each x_i maps this polynomial to $(1+x+\cdots+x^{p-1})^n$. This shows that level m of P_n consists of $u(m, n)$ monomials. Thus the result quoted above amounts to the following: *the longest antichain of P_n has size $M(p^n)$; and in particular $M(p^n) = \max u(m, n)$.*

We shall use this twice; first, in establishing that

$$(3.1)\qquad \frac{1}{p}M(p^{n+1}) \leqslant M(p^n) \leqslant \frac{2}{p+1}M(p^{n+1}) \quad \text{whenever } n>0.$$

By the definition of $u(m, n+1)$,

$$u(m, n+1) = \sum_{i=1}^{p} u(m-p+i, n):$$

hence

$$\begin{aligned} M(p^{n+1}) &= \sum_{i=1}^{p} u([(p-1)(n+1)/2]-p+i, n) \\ &\leqslant p \max u(m, n) = pM(p^n). \end{aligned}$$

This proves the first inequality. A simple manipulation of binomial coefficients proves the second when $p=2$, so consider the case $p = 2k+1$. Then

$$\begin{aligned} M(p^{n+1}) &= u(kn+k, n+1) \\ &= \sum u(kn-k-1+i, n) \\ &= \sum\sum u(kn-3k-2+i+j, n-1) \\ &\geqslant (k+1)\sum u(kn-2k-1+i, n-1) \\ &= (k+1)u(kn, n) \\ &= (k+1)M(p^n) \end{aligned}$$

proves the second inequality.

The second application of the de Bruijn *et al.* result is the following.

(3.2) Let $\mathbb{F}$ be a field of characteristic p and $\mathbb{F}C_p^n$ the group algebra of an elementary abelian group of order p^n. Each ideal of $\mathbb{F}C_p^n$ can be generated, as ideal, by $M(p^n)$ elements. The power $R^{[(p-1)n/2]}$ of the radical R is an ideal which cannot be generated by fewer than $M(p^n)$ elements.

We only sketch the proof. Let $g_1, \ldots, g_n$ generate C_p^n: then $x_i \mapsto g_i - 1$ defines a homomorphism of the polynomial algebra $\mathbb{F}[x_1, \ldots, x_n]$ onto $\mathbb{F}C_p^n$, with kernel the ideal generated by $x_1^p, \ldots, x_n^p$. Let us abuse

language by identifying each element of $\mathbb{F}C_p^n$ with its unique polynomial pre-image not involving any x_i^p, and then by viewing each of the polynomials as an $\mathbb{F}$-linear combination of the monomials in P_n. For each nonzero polynomial, consider the monomials which it involves (with nonzero coefficient); among these, take the first in lexicographic order, and call that the leading term of the polynomial. A routine argument shows that each ideal has a generating set consisting of polynomials whose leading terms are pairwise distinct and incomparable in the partial order by divisibility discussed above, so there are at most $M(p^n)$ of them. The radical R is generated by $x_1, \ldots, x_n$, and R^m is generated by level m of P_n; this level is independent modulo R^{m+1}, so R^m cannot be generated by fewer than $u(m, n)$ elements.

4. We now come to the critical step of this paper.

(4.1) LEMMA. *Let $\mathbb{F}$ be a field of characteristic p. If there is a finite p-group G and an $\mathbb{F}G$-module U of dimension p^n having a basis permuted transitively by G and having at least one trivial section of dimension t, then the regular $\mathbb{F}C_p^n$-module also has a trivial section of dimension t.*

Proof. For fixed n and t, let S denote the set of all pairs (G, U) satisfying the hypotheses: the claim is that if S is nonempty then $(C_p^n, \mathbb{F}C_p^n) \in S$. For each (G, U) in S, take a basis of U permuted transitively by G, and denote by G_U the stabilizer in G of one of the elements of that basis.

The proof is based on a construction which yields, for each (G, U) in S and for each maximal subgroup H of G containing G_U, an $\mathbb{F}(H \times C_p)$-module V such that $(H \times C_p, V) \in S$. Once we have such a construction, the lemma can be deduced as follows. Of all (G, U) in S, consider those with minimal $|G|$, and among these one with G having as large an elementary abelian direct factor as possible. Say, $G = C_p^a \times B$ with B having no direct factor of order p. The minimality of $|G|$ implies that G is faithful on U: thus if $B = 1$ then $U \cong \mathbb{F}G$, the only faithful transitive permutation representation of an abelian group being the regular one. It remains to show that $B > 1$ leads to a contradiction. If $B > 1$ then G has a maximal subgroup H containing C_p^a. The minimality of $|G|$ implies that no proper subgroup of G can act transitively on the chosen basis of U. As H-orbits correspond to G_U, H double cosets, the intransitivity of H demands that $G_U \leqslant H$. Now $C_p^a \leqslant H \leqslant C_p^a \times B$ yields that $H = C_p^a \times (H \cap B)$ so $H \times C_p \cong C_p^{a+1} \times (H \cap B)$, and thus $(H \times C_p, V) \in S$ contradicts the choice of (G, U).

To prepare for the construction, we need to analyse an arbitrary (G, U) in S in terms of a maximal subgroup H containing G_U. Let X/Y be a trivial section of dimension t in U. Since the G_U, H double cosets are

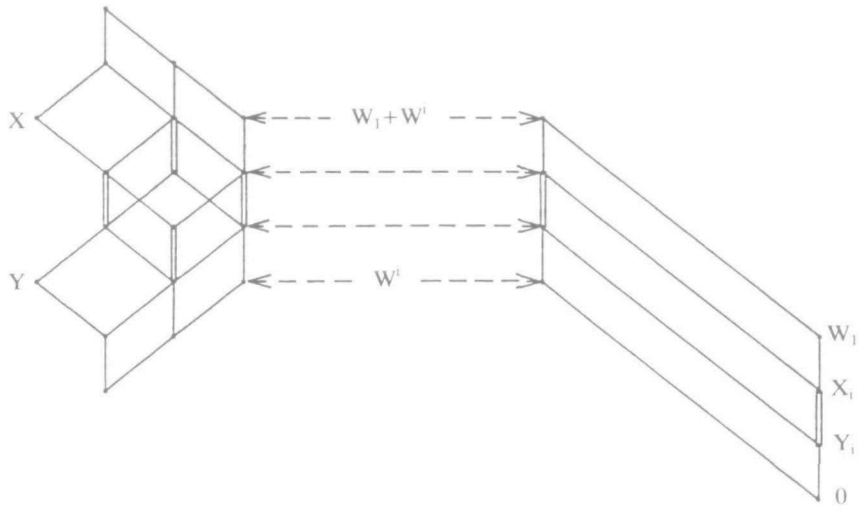

FIG. 1

just the p cosets modulo H, the chosen basis of U is permuted by H in p orbits: let $W_1, \ldots, W_p$ denote their $\mathbb{F}$-spans. As G itself acts transitively, an element g of G outside H must permute these orbits, and hence also the W_i, cyclically: say, $W_i g = W_{i+1}$ when $1 \leq i \leq p-1$ and $W_p g = W_1$. By the Isomorphism Theorem,

$$\frac{(X \cap W_1) + Y}{Y} \cong \frac{X \cap W_1}{(X \cap W_1) \cap Y} = \frac{X \cap W_1}{Y \cap W_1}.$$

This is a somewhat degenerate special case, at $i = 1$, of a general fact which holds for $i = 1, \ldots, p$. Define W^i by

$$W^1 = 0,\ W^2 = W_2,\ W^3 = W_2 + W_3,\ \ldots,\ W^p = W_2 + \cdots + W_p,$$

and set $X_i = (X + W^i) \cap W_1$, $Y_i = (Y + W^i) \cap W_1$. Figure 1 shows two sublattices of the submodule lattice of U_H (that is, of $\mathbb{F}H$-submodules of U): the first is the sublattice generated by X, Y, $W_1 + W^i$, and W^i, while the second is that generated by W^i, W_1, X_i, and Y_i. [As is well known, *every* modular lattice generated by two 2-element chains "looks like" (a possibly degenerate form of) the first picture.] Repeated applications of the Isomorphism Theorem gives that, for $i = 1, \ldots, p$,

$$\frac{[X \cap (W_1 + W^i)] + Y}{(X \cap W^i) + Y} \cong \frac{X_i}{Y_i}. \tag{4.2.i}$$

Since X/Y is a trivial G-module, each subspace of X containing Y is

g-invariant; in particular,

$$[X \cap (W_1 + W^i)] + Y = [X \cap (W_1 g + W^i g)] + Y,$$

so

$$[X \cap (W_1 + W^i)] + Y = \begin{cases} (X \cap W^{i+1}) + Y & \text{if } i < p, \\ X & \text{if } i = p. \end{cases} \tag{4.3}$$

This shows that the dimensions of the left hand sides of (4.2.1), . . . , (4.2.p) sum to dim X/Y, whence also

$$\sum \dim X_i/Y_i = t. \tag{4.4}$$

On the other hand,

$$X_i \leqslant Y_{i+1} \quad \text{whenever } i < p \tag{4.5}$$

because

$$\begin{aligned} (X + W^i) \cap W_1 &\leqslant (X + W^i) \cap (W_1 + W^i) \\ &\leqslant [X \cap (W_1 + W^i)] + W^i && \text{by modularity,} \\ &\leqslant [X \cap (W_1 + W^i)] + Y + W^i \\ &\leqslant (X \cap W^{i+1}) + Y + W^i && \text{by (4.3)} \\ &\leqslant Y + W^{i+1}. \end{aligned}$$

This completes the analysis. For the case $p = 5$, the conclusions are summarised in Figure 2.

The construction is now a fairly straightforward matter. Let V be the $H \times C_p$-module induced from the H-module W_1. Transitive permutation modules induce to transitive permutation modules, and $\dim V = p \dim W_1 = \dim U = p^n$ as required. It remains to show that V does have a trivial section of dimension t. To this end, view V as the outer tensor product $W_1 \# \mathbb{F}C_p$ of the $\mathbb{F}H$-module W_1 and the regular $\mathbb{F}C_p$-module (every module induced from a direct factor is such an outer tensor product). Let J denote the radical of $\mathbb{F}C_p$, and use the convention $J^0 = \mathbb{F}C_p$. We claim that

$$\bar{X} = \sum X_i \# J^{i-1}, \qquad \bar{Y} = \sum Y_i \# J^{i-1}$$

gives a trivial section $\bar{X}/\bar{Y}$ of dimension t in V. Since $X_i \geqslant Y_i$, we certainly have that $\bar{X} \geqslant \bar{Y}$. As H acts trivially on each X_i/Y_i (because the isomorphisms (4.2.i) are H-isomorphisms), we also have that

$$[\bar{X}, H] = \sum [X_i \# J^{i-1}, H] = \sum [X_i, H] \# J^{i-1} \leqslant \sum Y_i \# J^{i-1} = \bar{Y}.$$

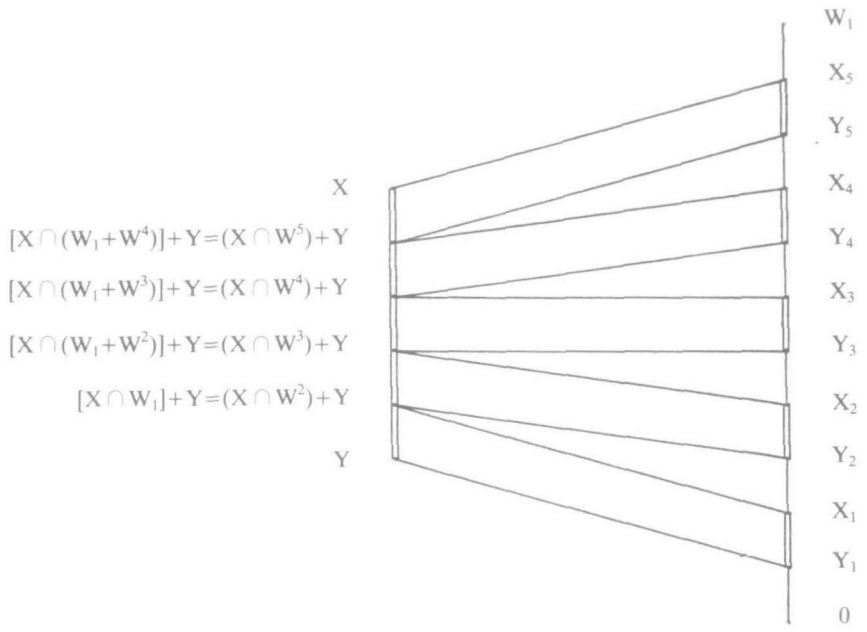

FIG. 2

On the other hand, using $J^p = 0$ and (4.5) we get

$$[\bar{X}, C_p] = \sum [X_i \# J^{i-1}, C_p] = \sum X_i \# [J^{i-1}, C_p] = \sum X_i \# J^i$$
$$\leqslant \sum Y_{i+1} \# J^i \leqslant \bar{Y}.$$

So $H \times C_p$ acts trivially on $\bar{X}/\bar{Y}$, and all that remains is a dimension count. Let $z_0, \ldots, z_p$ be a basis for $\mathbb{F}C_p$ chosen so that $z_i, \ldots, z_p$ spans J^{i-1}: then one may, as usual, write $V = \bigoplus (W_1 \otimes z_j)$; in that language,

$$X_i \# J^{i-1} = \bigoplus_{j \geqslant i} (X_i \otimes z_j)$$

whence $\bar{X} = \bigoplus (X_i \otimes z_i)$, so $\dim \bar{X} = \sum \dim X_i$. Similarly $\dim \bar{Y} = \sum \dim Y_i$, and so by (4.4) one gets $\dim \bar{X}/\bar{Y} = t$ as required.

5. The proofs of the group-theoretic components of the Theorem are now immediate.

Proof of (2.4). Let G be the semidirect product of C_p^{n-1} and R^m where R is the radical of the group algebra $\mathbb{F}_p C_p^{n-1}$ (over the field $\mathbb{F}_p$ of p

elements) and $m = [(p-1)(n-1)/2]$. The commutator subgroup G' is R^{m+1}, so G/G' is $C_p^{n-1} \times R^m/R^{m+1}$: by (3.2), this elementary abelian quotient of G has rank $(n-1) + M(p^{n-1})$. On the other hand, there is only one minimal ideal in the group algebra $\mathbb{F}_p C_p^{n-1}$ and so only one minimal $\mathbb{F}_p C_p^{n-1}$-submodule in R^m; a subspace-complement G_0 to that submodule in R^m has codimension 1 in R^m and so index p^n in G. This G_0 is corefree in G, so the natural transitive representation of G on the set of its cosets modulo G_0 is faithful.

Proof of (2.5). Let K be any transitive p-group of degree p^n, and K_0 a point stabilizer in K: then K_0 is a corefree subgroup of index p^n. Since K is a p-group, there is a subgroup H such that $K_0 \lhd H \leqslant K$ and $|H : K_0| = p$. By the Embedding Theorem (see Théorème 1 in § 4 of Krasner and Kaloujnine [4]), K embeds (as permutation group) in the permutational wreath product $C_p \operatorname{wr} G$ where G is the group of the permutations induced by K on the set of its cosets modulo H (so in particular G is a transitive p-group of degree p^{n-1}). Moreover, if U denotes the base group of this wreath product then $KU = GU$. Set $U \cap K = X$ and $U \cap \Phi(K) = Y$ (as usual, we write $\Phi(K)$ for the Frattini subgroup of K): then $K/X \cong KU/U \cong G$ so $K/X\Phi(K) \cong G/\Phi(G)$ and $X\Phi(K)/\Phi(K) \cong X/Y$ whence

$$|K/\Phi(K)| = |G/\Phi(G)|\,|X/Y|.$$

Set $\dim X/Y = t$: by (4.1), the regular $\mathbb{F}_p C_p^{n-1}$-module also has a trivial section of dimension t, so by (3.2) we have $t \leqslant M(p^{n-1})$. This shows that the rank of $K/\Phi(K)$ is at most $f(p^{n-1}) + M(p^{n-1})$, as required.

Proof of (2.1). The first inequality follows directly from (2.4) and the first half of (3.1). The second inequality is proved by induction on n. The initial step is provided by direct calculation: $f(p^2) = 2$, while $M(p^2)$ is p. The inductive step is simple:

$$\begin{aligned} f(p^n) &\leqslant f(p^{n-1}) + M(p^{n-1}) && \text{by (2.5)} \\ &\leqslant \left(\frac{2}{p-1} + 1\right) M(p^{n-1}) && \text{by the inductive hypothesis,} \\ &\leqslant \frac{2}{p-1} M(p^n) && \text{by the second half of (3.1).} \end{aligned}$$

6. We owe the first step towards the asymptotic expression (2.2) for $M(p^n)$ to Professor Kurt Mahler. We need only consider the case when p is odd, say $p = 2k+1$. Set

$$F(x) = \left(\sum_{j=-k}^{k} x^j\right)^n = \sum_{j=0}^{kn} a_j(x^{-j} + x^j):$$

then $M(p^n) = 2a_0$. Now

$$F(e^{i\theta}) = (1 + 2\cos\theta + \cdots + 2\cos k\theta)^n = \sum_{j=0}^{kn} 2a_j \cos j\theta.$$

Since

$$1 + 2\cos\theta + \cdots + 2\cos k\theta = \frac{\sin p\theta/2}{\sin \theta/2},$$

it follows that

$$\frac{M(p^n)}{p^n} = \frac{1}{2\pi}\int_{-\pi}^{\pi} \left(\frac{\sin p\theta/2}{p \sin \theta/2}\right)^n d\theta = \frac{2}{\pi}\int_0^{\pi/2} \left(\frac{\sin pu}{p \sin u}\right)^n du.$$

Thus what we need is an asymptotic formula for the last integral: we leave that for the last section. Essentially the same argument shows this equation also holds for $p = 2$ and n even.

Here we show how to deduce (2.3). It is easily shown in the next section that

$$\left|\frac{\sin pu}{p \sin u}\right| < 2^{-\frac{1}{2}} \quad \text{for } \pi/2p \leq u \leq \pi/2.$$

Since $u^{-1}\sin u$ is decreasing on the interval $(0, \pi/2)$ and $p \geq 2$,

$$\frac{\sin pu}{p \sin u} = \frac{\sin pu}{pu}\frac{2u}{\sin 2u}\cos u \leq \cos u \quad \text{for } 0 \leq u \leq \pi/2p.$$

Hence

$$\int_0^{\pi/2} \left(\frac{\sin pu}{p \sin u}\right)^n du \leq \int_0^{\pi/2p} (\cos u)^n du + \frac{\pi}{2} 2^{-n/2}.$$

Using

$$\int_0^{\pi/2} (\cos u)^n du \leq \sqrt{2/(n+1)}$$

gives (2.3) except for $p = 2$ and n odd; but then $M(2^n) = (M(2^{n+1}))/2$ and (2.3) also holds in this case.

7. Professor Sir Peter Swinnerton-Dyer happened to be passing through Canberra just at the right time and he kindly provided us with the asymptotic formula

$$\int_0^{\pi/2} \left(\frac{\sin pu}{p \sin u}\right)^n du = n^{-\frac{1}{2}}\sqrt{3\pi/2(p^2-1)} + O(n^{-\frac{3}{2}}): \tag{7.1}$$

in the light of the foregoing, this completes the proof of (2.2). His proof of (7.1) is reproduced below.

It will eventually appear that

$$\int_0^{\pi/2} \left(\frac{\sin pu}{p \sin u}\right)^n \mathrm{d}u$$

is precisely of order $n^{-\frac{1}{2}}$, so in estimating it we can certainly throw away terms which are $o(n^{-1})$.

We know that $u^{-1} \sin u$ is strictly monotone decreasing in $(0, \pi/2)$. As a first step this gives in $\pi/2p \leqslant u \leqslant \pi/2$

$$\left|\frac{\sin pu}{p \sin u}\right| \leqslant \frac{1}{p \sin u} \leqslant \frac{1}{p \sin \pi/2p} \leqslant \frac{2}{\pi}\left(\frac{\sin \pi/2p}{\pi/2p}\right)^{-1}$$
$$\leqslant \frac{2}{\pi}\left(\frac{\sin \pi/4}{\pi/4}\right)^{-1} \quad \text{since } \pi/2p \leqslant \pi/4$$

and this is equal to $2^{-\frac{1}{2}}$. So the contribution to the integral from $\pi/2p \leqslant u \leqslant \pi/2$ is exponentially small and in particular is $o(n^{-1})$.

In $0 < u < \pi/2p$ we have

$$\frac{\mathrm{d}}{\mathrm{d}u}\left(\frac{\sin pu}{p \sin u}\right) = \frac{p \cos pu \sin u - \sin pu \cos u}{p \sin^2 u}$$

which clearly has the same sign as

$$\frac{\tan u}{u} - \frac{\tan pu}{pu}.$$

But $y^{-1} \tan y$ is monotone increasing in $0 < y < \pi/2$, so the last displayed expression is negative and

$$\frac{\sin pu}{p \sin u} \quad \text{is monotone decreasing in } 0 < u < \pi/2p.$$

Its value at $u = n^{-\frac{1}{3}}$ is

$$1 - \tfrac{1}{6}(p^2 - 1)n^{-\frac{2}{3}} + O(n^{-\frac{4}{3}})$$

using the power series for sin, so it lies between this and zero in $n^{-\frac{1}{3}} < u < \pi/p$. In that interval we therefore have

$$0 \leqslant \left(\frac{\sin pu}{p \sin u}\right)^n \leqslant \{1 - \tfrac{1}{6}(p^2 - 1)n^{-\frac{2}{3}} + O(n^{-\frac{4}{3}})\}^n$$
$$= \exp n\{-\tfrac{1}{6}(p^2 - 1)n^{-\frac{2}{3}} + O(n^{-\frac{4}{3}})\} \leqslant \exp\{-\tfrac{1}{12}(p^2 - 1)n^{\frac{1}{3}}\}$$

say, which is certainly $o(n^{-1})$; so this interval too contributes $o(n^{-1})$ to the integral.

There remains the interval $0 < u < n^{-\frac{1}{3}}$. In this we have

$$\left(\frac{\sin pu}{p \sin u}\right)^n = \{1 - \tfrac{1}{6}(p^2-1)u^2 + O(u^4)\}^n = \exp n\{-\tfrac{1}{6}(p^2-1)u^2 + O(u^4)\}$$
$$= \exp\{-\tfrac{1}{6}(p^2-1)nu^2 + O(n^{-\frac{1}{3}})\}$$
$$= (1 + O(n^{-\frac{1}{3}}))\exp\{-\tfrac{1}{6}(p^2-1)nu^2\}$$
$$= \exp\{-\tfrac{1}{6}(p^2-1)nu^2\} + O(n^{-\frac{1}{3}}).$$

Hence

$$\int_0^{\pi/2} \left(\frac{\sin pu}{p \sin u}\right)^n du = \int_0^{n^{-\frac{1}{3}}} \left(\frac{\sin pu}{p \sin u}\right)^n du + O(n^{-1})$$
$$= \int_0^{n^{-\frac{1}{3}}} \exp\{-\tfrac{1}{6}(p^2-1)nu^2\}\, du + O(n^{-\frac{2}{3}})$$
$$= n^{-\frac{1}{2}}a^{-1} \int_0^{n^{\frac{1}{6}}a} e^{-y^2}\, dy + O(n^{-\frac{2}{3}})$$

where $6a^2 = p^2 - 1$

$$= n^{-\frac{1}{2}}a^{-1} \int_0^{\infty} e^{-y^2}\, dy + O(n^{-\frac{2}{3}})$$

since what the additional range of integration contributes is exponentially small. But it is well known that

$$\int_0^{\infty} e^{-y^2}\, dy = \tfrac{1}{2}\pi^{\frac{1}{2}}$$

so we have

$$\int_0^{\pi/2} \left(\frac{\sin pu}{p \sin u}\right)^n du = n^{-\frac{1}{2}}\sqrt{3\pi/2(p^2-1)} + O(n^{-\frac{2}{3}}).$$

Of course the error term is really $O(n^{-1+\varepsilon})$ for any $\varepsilon > 0$.

REFERENCES

1. Martin Aigner, *Combinatorial theory*, Springer-Verlag, Berlin Heidelberg New York, 1979.
2. Muhammed Salihu Audu, 'Transitive permutation groups of prime-power order', D.Phil. thesis, Oxford, 1983.
3. N. G. de Bruijn, Ca. van Ebbenhorst Tengbergen, and D. Kruyswijk, 'On the set of divisors of a number', *Nieuw Arch. Wiskunde* (2) 23 (1951), 191–193; MR 13-207.

4. Marc Krasner et Leo Kaloujnine, 'Produit complet des groupes de permutations et problème d'extension de groupes. II', *Acta. Sci. Math. Szeged* 14 (1950), 39–66.
5. Christian Ronse, 'On permutation groups of prime power order', *Math. Z.* 173 (1980), 211–215.

Department of Mathematics, I.A.S.
Australian National University
G.P.O. Box 4
Canberra, A.C.T., 2601
Australia